IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications;

(d) executing a pattern for testing the potentially malicious content network communications for malicious code; and

(e) conditionally delivering the network communications over the network based on the testing;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

2. (Original) The method as recited in claim 1, further comprising scanning the network communications for known malicious content.

3. (Original) The method as recited in claim 1, wherein the malicious content includes a mass-mailer virus.

4. (Original) The method as recited in claim 1, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

5. (Original) The method as recited in claim 1, wherein the network communications include electronic mail messages.

6. (Original) The method as recited in claim 5, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

7. (Cancelled)

8. (Currently Amended) The method as recited in claim 1, further comprising cleaning the potentially malicious content if malicious code is found, which is[for] disabling [the]of malicious code.

9. (Currently Amended) A computer program product embodied on a computer readable medium for network-based scanning for potentially malicious content, comprising:

(a) computer code that monitors network communications over a network;

(b) computer code that identifies potentially malicious content in the network communications;

(c) computer code that quarantines the potentially malicious content of the network communications;

(d) computer code that executes a pattern for testing the potentially malicious content network communications for malicious code; and

(e) computer code that conditionally delivers the network communications over the network based on the testing;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

10. (Currently Amended) A system for network-based scanning for potentially malicious content, comprising:

(a) logic that monitors network communications over a network;

(b) logic that identifies potentially malicious content in the network communications;

(c) logic that quarantines the potentially malicious content of the network communications;

(d) logic that executes a pattern for testing the potentially malicious content network communications for malicious code; and

(e) logic that conditionally delivers the network communications over the network based on the testing;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

11. (Currently Amended) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications; and

(d) delivering the network communications over the network after a predetermined delay;

wherein the delay is for allowing quarantining of the potentially malicious content until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

12. (Original) The method as recited in claim 11, further comprising scanning the network communications for known malicious content.

13. (Original) The method as recited in claim 11, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

14. (Original) The method as recited in claim 11, wherein the network communications include electronic mail messages.

15. (Original) The method as recited in claim 14, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

16. (Cancelled)

17. (Currently Amended) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications in a quarantine; and

(d) delivering the network communications from the quarantine over the network in response to a request from a user;

wherein it is determined whether the user is authorized, and the network communications are delivered only if the user is determined to be authorized.

18. (Original) The method as recited in claim 17, wherein the user is an intended recipient of the quarantined network communications.

19. (Original) The method as recited in claim 17, further comprising scanning the network communications for known malicious content.

20. (Original) The method as recited in claim 17, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

21. (Original) The method as recited in claim 17, wherein the network communications include electronic mail messages.

22. (Original) The method as recited in claim 21, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

23. (Currently Amended) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring incoming and outgoing network communications over a network at a gateway;

(b) scanning the network communications for known malicious content;

(c) identifying potentially malicious content in the network communications;

(d) wherein content is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value;

(e) wherein the network communications include electronic mail messages, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line passing through the network for a given period of time is greater than a predetermined value;

(f) quarantining the potentially malicious content of the network communications;

(g) delivering the network communications over the network upon occurrence of the first of:

(i) scanning the potentially malicious content with a malicious code detection file received after the potentially malicious content is received;

(ii) upon receiving a user request;

(iii) upon passage of a predetermined amount of time;

(h) notifying an intended recipient of the potentially malicious content that the potentially malicious content has been quarantined;

(i) notifying a sender of the potentially malicious content that the potentially malicious content has been quarantined; and

(j) cleaning the potentially malicious content if malicious code is found, which is[for] disabling [the]of malicious code.

24. (New) The method as recited in claim 1, wherein the potentially malicious content is identified utilizing heuristics.

25. (New) The method as recited in claim 24, wherein the heuristics include generating a histogram of content that has been sent over the network during a period of time and analyzing the histogram to determine whether a number of copies of the potentially malicious content that have been sent over the network during the period of time exceed a predetermined value.

26. (New) The method as recited in claim 1, wherein the quarantining includes containing the potentially malicious content and preventing the potentially malicious content from creating damage.

27. (New) The method as recited in claim 1, wherein when multiple recipients are to receive a copy of the potentially malicious content over the network, a single copy of the potentially malicious content is quarantined and each of the recipients is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients.

28. (New) The method as recited in claim 1, wherein an intended recipient of the network communications is notified that the potentially malicious content is quarantined.